

WHAT IS CLAIMED IS:

1. A method for securely storing a public
key for encryption of data in a computing device,
5 the method using a user-specific key pair which is
securely stored in the computing device, the method
comprising:

a receiving step of receiving a target
public key corresponding to a target device;

10 an obtaining step of obtaining a user-
specific key pair from a secure registry;

a key encrypting step of using a user-
specific private key from the user-specific key pair
to create a target key verifier based on the target
15 public key;

a storing step of storing the target key
verifier and the target public key in a storage
area;

a retrieving step of retrieving the target
20 key verifier and the target public key from the
storage area;

a verification step of applying a user-
specific public key from the user-specific key pair
to the target key verifier for verifying the
25 authenticity of the target public key; and

a data encrypting step of encrypting data
with the target public key, in the case that the
authenticity of the target public key is verified,
thereby creating encrypted data for transmission to
30 the target device.

2. A method according to Claim 1, wherein the user-specific key pair is obtained from a key function call which is supported by an operating system executing in the computing device.

5

3. A method according to Claim 2, wherein the operating system securely maintains a user-specific key pair for each of a plurality of users of the computing device.

10

4. A method according to Claim 3, wherein each user-specific key pair can only be accessed by providing the operating system with user identification data corresponding to the user-specific key pair.

15

5. A method according to Claim 1, wherein the target key verifier created in the key encrypting step is an encrypted version of the target public key.

20

6. A method according to Claim 5, wherein the target key verifier is created by encrypting the target public key with the user-specific private key using an encryption algorithm.

25

7. A method according to Claim 5, wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm.

30

10010974-120504

8. A method according to Claim 7, wherein
the verification step further includes using a key
verification algorithm to compare the decrypted
target key verifier to the target public key for
5 verifying the authenticity of the target public key.

9. A method according to Claim 8, wherein
the verification step is performed by a verification
function call which is supported by an operating
10 system executing in the computing device.

10. A method according to Claim 1, wherein
the target key verifier created in the key
encrypting step is a digital signature of the target
15 public key.

11. A method according to Claim 10,
wherein the digital signature of the target public
key is created by applying a hashing algorithm to
20 the target public key to obtain a target key hash,
and then encrypting the target key hash with the
user-specific private key using an encryption
algorithm.

12. A method according to Claim 10,
wherein the digital signature of the target public
key is created by applying a hashing algorithm to
25 the target public key to obtain a target key hash,
and then subjecting the target key hash to a
30 security algorithm.

13. A method according to Claim 12,
wherein the verification step includes decrypting
the target key verifier with the user-specific
public key using a decryption algorithm to obtain a
5 decrypted target key hash.

14. A method according to Claim 13,
wherein the verification step further includes
reapplying a hashing algorithm to the target public
10 key to obtain a new target key hash and using a hash
verification algorithm to compare the decrypted
target key hash to the new target key hash for
verifying the authenticity of the target public key.

15. A method according to Claim 14,
wherein the verification step is performed by a
verification function call which is supported by an
operating system executing in the computing device.

16. A method according to Claim 1, wherein
the receiving step includes applying a hashing
algorithm to the received target public key to
obtain a received target key hash and using a hash
verification algorithm to compare the received
25 target key hash to a test target key hash for
verifying the authenticity of the received target
public key.

17. A method according to Claim 16,
30 wherein the test target key hash is input by a user.

18. A method according to Claim 17,
wherein the target device is a printer and wherein
the test target key hash is obtained from a test
page printed by the printer.

5

19. A method according to Claim 1, wherein
the target device is a printer and the target public
key is a printer public key.

10

20. A method according to Claim 19,
wherein, in the receiving step, the printer public
key is received in response to a key request sent to
the printer.

15

21. A method according to Claim 19,
wherein the method is performed in a printer driver
executing on the computing device.

20

22. A method for securely storing a
printer public key for encryption of print data in a
computing device, the method using a user-specific
key pair which is securely stored in the computing
device, the method comprising:

25

a receiving step of receiving a printer
public key corresponding to a printer;

an obtaining step of obtaining a user-
specific key pair from a secure registry upon
receipt of a corresponding user identification;

30

a first hashing step of applying a hashing
algorithm to the printer public key to create a
first printer key hash;

an encryption step of applying an encryption algorithm to encrypt the first printer key hash with a user-specific private key from the user-specific key pair, thereby creating a printer key signature;

a storing step of storing the printer key signature and the printer public key in a storage area;

a retrieving step of retrieving the printer key signature and the printer public key from the storage area;

a second hashing step of applying the hashing algorithm to the retrieved printer public key to create a second printer key hash;

a decrypting step of applying a decryption algorithm to decrypt the printer key signature with a user-specific public key from the user-specific key pair, thereby retrieving the first printer key hash;

a verification step of applying a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the retrieved printer public key; and

a print data encrypting step of applying an encryption algorithm to print data using the retrieved printer public key, in the case that the authenticity of the retrieved printer public key is verified, to create encrypted print data for transmission to the printer.

a processor for executing the process steps stored in said program memory.

5 25. Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for authenticating a public key for encryption of data, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 23.

10

 26. A computer-readable medium which stores computer-executable process steps, the computer-executable process steps to authenticate a public key for encryption of data, said computer-executable process steps comprising process steps executable to perform a method according to any of
15 Claims 1 to 23.

205027426001